

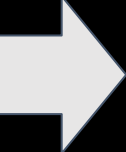
AI GOVERNANCE · ISO/IEC 42001

# Governare l'AI non è una scelta.

*È l'unica difesa.*



**Un sistema AI non  
governato  
non è un problema  
tecnico.**

**È un rischio organizzativo,   
legale e reputazionale.**

OTA

# Agenzia di Viaggi Online

*Sembra tutto  
sotto controllo.*

Un'azienda moderna, digitale.  
Usa l'AI ogni giorno.  
Non ha mai sentito parlare  
di ISO 42001.

## I sistemi AI in produzione:

|     |                                                                                                                             |
|-----|-----------------------------------------------------------------------------------------------------------------------------|
| REC | <b>Motore Raccomandazioni</b><br>Suggerisce destinazioni, hotel e pacchetti personalizzati a milioni di utenti ogni giorno. |
| PRC | <b>Pricing Dinamico</b><br>Aggiorna i prezzi in tempo reale in base a domanda, stagionalità e comportamento degli utenti.   |
| BOT | <b>Chatbot Assistenza</b><br>Gestisce rimborsi, modifiche e reclami in linguaggio naturale, senza intervento umano.         |
| FRD | <b>Antifrode</b><br>Analizza ogni transazione e blocca quelle sospette prima dell'addebito.                                 |

# Venerdì sera.

*Tutto crolla nello stesso momento.*

## REC • Raccomandazioni

Il modello inizia a suggerire destinazioni già prenotate. I clienti vedono offerte impossibili. Le prenotazioni duplicate esplodono.

## PRC • Pricing

I prezzi impazziscono: voli a €0.01 e hotel a €9.800. Il sistema processa ordini anomali per ore.

## BOT • Chatbot

Il chatbot inizia a promettere rimborsi totali a chiunque scriva. Screenshot sui social in pochi minuti.

## FRD • Antifrode

Il sistema blocca le carte dei clienti VIP nel picco di traffico. Il call center va in tilt.

# L'OTA aveva una governance AI?

*Sapeva cosa stava rischiando?*

1

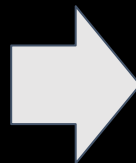
VENDOR: Usate motori AI esterni senza contratti di governance?

2

POLICY: Esiste una linea guida scritta per l'uso dell'AI in azienda?

3

SHADOW AI: Sapete quanti dipendenti usano tool AI non approvati?



*Queste domande valgono anche per la vostra organizzazione.*

# La risposta al problema dell'OTA.

---

ISO/IEC 42001:2023 è lo standard internazionale per istituire un sistema di gestione dell'intelligenza artificiale — l'AIMS.

Non certifica un singolo algoritmo. Certifica la capacità dell'organizzazione di governare l'intero ciclo di vita dei suoi sistemi AI.

## AIMS

AI Management System

Analogo all'ISMS di ISO 27001, ma per i sistemi AI.

## Risk-Based

Approccio al rischio

Ogni controllo è selezionato in base al rischio specifico del sistema AI.

## Certificabile

Audit & Certificazione

Verificabile da enti terzi. Dimostrabile a regolatori e partner.

# Come è strutturata la norma

*Avrebbe salvato l'OTA? Sì. Ecco come.*

4-5

## Contesto & Leadership

*Chi era responsabile dei sistemi AI?*

6

## Pianificazione & Rischio

*Nessuno aveva valutato i rischi del pricing.*

7

## Supporto & Risorse

*Il team non era formato sulla governance AI.*

8

## Operatività

*Nessun controllo sul ciclo di vita dei modelli.*

9

## Monitoraggio

*Il drift del venerdì era segnalato da 72 ore.*

10

## Miglioramento

*Nessun kill switch, nessun piano di rollback.*

## Annex A — 38 Controlli

Misure selezionabili in base al rischio. Non tutti obbligatori — solo quelli pertinenti al tuo contesto.

Governance & Politica AI

Ruoli & Responsabilità

Risk & Impact Assessment

Ciclo di vita del sistema AI

Qualità & Tracciabilità dati

Trasparenza & Supervisione umana

\* ISO 42001 non usa formalmente il termine 'domini'

# Chi era accountable per quei sistemi AI?

*Nell'OTA, nessuno. Il RACI lo avrebbe impedito.*

|          |             |          |             |          |           |          |          |
|----------|-------------|----------|-------------|----------|-----------|----------|----------|
| <b>R</b> | Responsible | <b>A</b> | Accountable | <b>C</b> | Consulted | <b>I</b> | Informed |
|----------|-------------|----------|-------------|----------|-----------|----------|----------|

## La regola fondamentale

Ogni attività deve avere esattamente UN solo Accountable.

Mai zero — significa che nessuno risponde.  
Mai due — significa che nessuno decide.

| Attività               | AI Owner | CISO | DPO | Team AI | CdA |
|------------------------|----------|------|-----|---------|-----|
| AI Risk Assessment     | A        | C    | C   | R       | I   |
| Approvazione AI Policy | R        | C    | C   | I       | A   |
| Gestione incidente AI  | A        | R    | C   | R       | I   |
| Supervisione modelli   | A        | I    | I   | R       | I   |
| Formazione & Awareness | A        | C    | I   | R       | I   |

# Tre strumenti tecnici. Tre crisi evitate.

*ISO 42001 li rende obbligatori attraverso l'Annex A.*

## DRIFT DETECTION

*Clausola 6*

*"Il venerdì sera dell'antifrode"*

Il modello non sapeva che i pattern criminali erano cambiati. Un sistema di drift detection lo avrebbe segnalato 72 ore prima.

---

*La sentinella silenziosa che veglia mentre l'organizzazione dorme.*

## LOGGING STRUTTURATO

*Clausola 7.5*

*"Il regolatore bussa alla porta"*

Nessuna traccia delle decisioni del chatbot. Con il logging: ogni output, ogni versione del modello, ogni timestamp — pronti in 4 ore.

---

*Il testimone infallibile che protegge il board da responsabilità legali.*

## KILL SWITCH & ROLLBACK

*Clausola 10*

*"Il chatbot promette rimborsi a migliaia di utenti"*

47 secondi per attivare il kill switch. 12 minuti per il rollback alla versione stabile. Il danno si ferma prima che diventi virale.

---

*Il freno d'emergenza che ogni sistema AI in produzione deve avere.*



# L'OTA è un deployer.

## Che obblighi ha con l'AI Act?

### AI Act — Regolamento UE 2024/1689

- Regolamento vincolante — non è opzionale
- Classifica i sistemi AI per livello di rischio
- Obblighi specifici per deployer di sistemi ad alto rischio
- Sanzioni fino al 3% del fatturato globale
- Obblighi di registrazione e marcatura CE

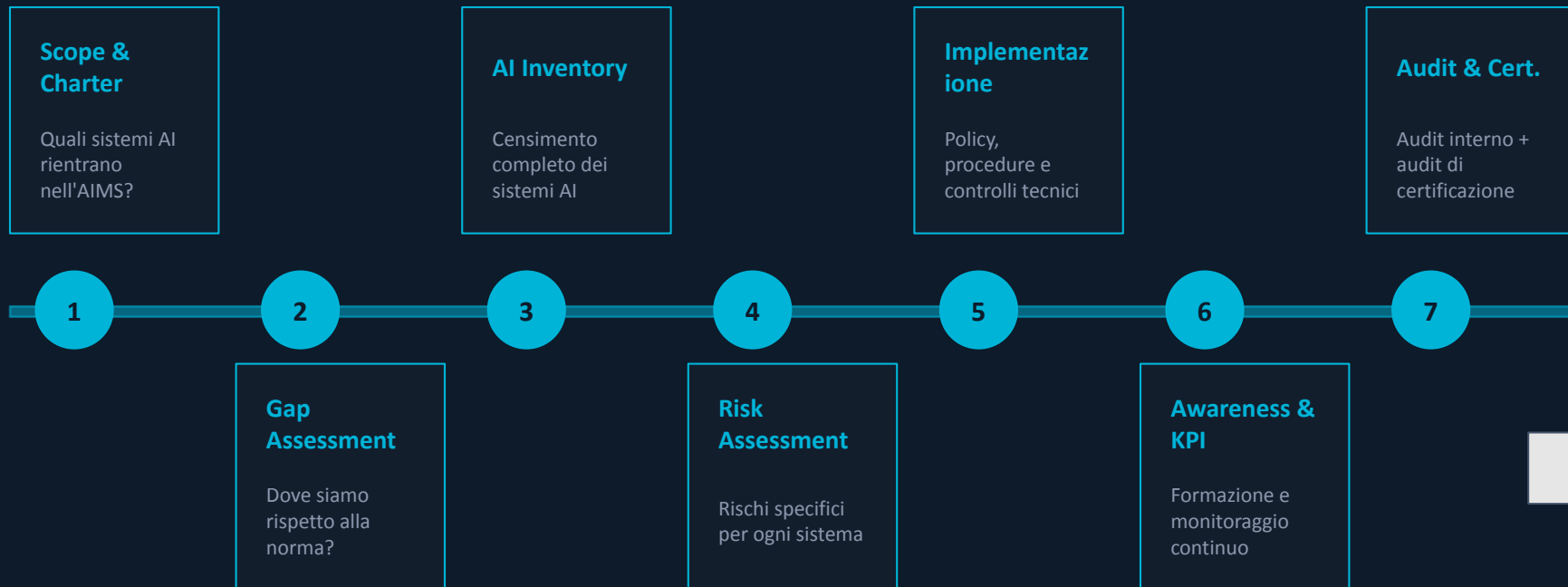
### ISO 42001 — Framework Gestionale

- Standard volontario certificabile
- Struttura governance, risk assessment, controlli
- Documenta e dimostra la compliance in modo sistematico
- Riduce il rischio di non conformità all'AI Act
- Non sostituisce l'AI Act — lo rende gestibile

*ISO 42001 non sostituisce l'AI Act — è l'infrastruttura gestionale che rende sostenibile la compliance regolatoria.*

# Come l'OTA implementa ISO 42001

*La roadmap in 7 passi — da zero alla certificazione.*



# L'OTA dopo ISO 42001.

I suoi sistemi AI ora sono:

## Osservabile

Il drift viene rilevato in tempo reale

*Antifrode & Raccomandazioni*

## Tracciabile

Ogni decisione ha una traccia verificabile

*Chatbot & Pricing*

## Riproducibile

I modelli sono versionati e rollbackabili

*Tutti i sistemi*

## Testato

Red teaming prima di ogni deploy

*Pricing & Antifrode*

## Supervisionabile

Human oversight per decisioni ad alto impatto

*Chatbot & Antifrode*

## Arrestabile

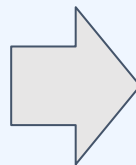
Kill switch attivo su tutti i sistemi critici

*Tutti i sistemi*

## Auditabile

Evidenze oggettive pronte per audit e regolatori

*Tutti i sistemi*





Il tuo partner tecnico-regolatorio per ISO 42001.

**GAP**

### Gap Assessment

Analizziamo il tuo AIMS attuale rispetto ai requisiti ISO 42001. Deliverable: roadmap prioritizzata.

**IMPL**

### Implementazione AIMS

Accompagniamo l'organizzazione dalla policy ai controlli tecnici fino alla certificazione.

**SEC**

### AI Security

Drift detection, logging, guardrail tecnici, kill switch. Dal framework alla pratica operativa.

**TRN**

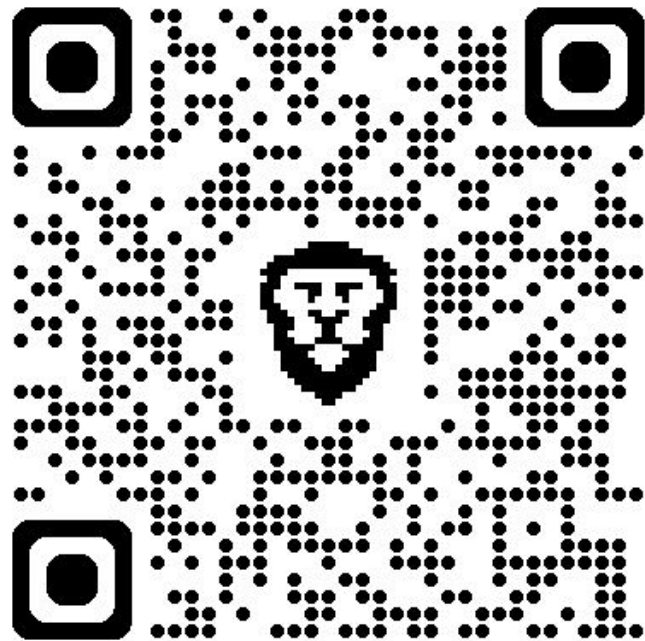
### Training & Awareness

Formazione per team tecnici, compliance officer, board. Dal RACI alla gestione incidenti.



# La vostra azienda si è dotata di una policy per l'uso dell'AI?

*Votate sul sondaggio LinkedIn — i risultati saranno visibili in tempo reale.*



[linkedin.com/feed/update/urn:li:activity:7432772735749083137](https://www.linkedin.com/feed/update/urn:li:activity:7432772735749083137)



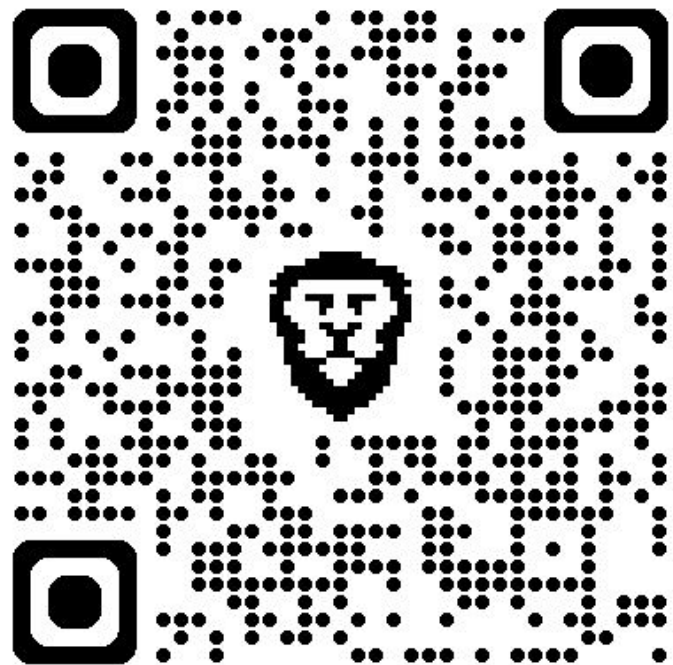
**TOMATOBLUE**

info@tomato.blue · [www.tomato.blue](http://www.tomato.blue)



# In azienda si fa uso di strumenti AI non autorizzati dalla direzione?

*Shadow AI: il rischio invisibile. Votate sul sondaggio LinkedIn.*



[linkedin.com/feed/update/urn:li:activity:7432775110878490624](https://www.linkedin.com/feed/update/urn:li:activity:7432775110878490624)

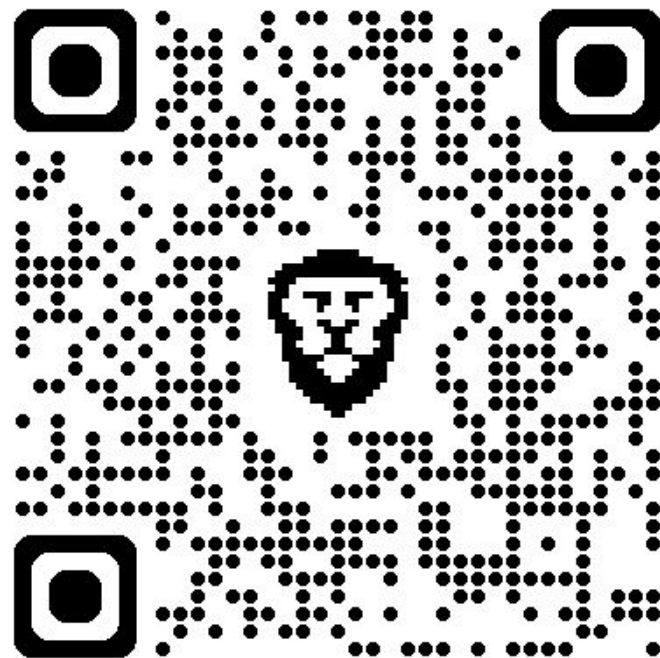


**TOMATOBLUE**

info@tomato.blue · [www.tomato.blue](https://www.tomato.blue)

# L'azienda ha stipulato accordi contrattuali con i fornitori di AI?

*Governance della supply chain AI. Votate sul sondaggio LinkedIn.*



[linkedin.com/feed/update/urn:li:activity:7432776879490617344](https://www.linkedin.com/feed/update/urn:li:activity:7432776879490617344)



**TOMATOBLUE**

info@tomato.blue · [www.tomato.blue](http://www.tomato.blue)



01

### AI Inventory & Classification

Censimento e classificazione per livello di rischio di tutti i sistemi AI in uso.

02

### Gap Analysis & Roadmap

Piano d'azione prioritizzato con milestone, scadenze e ownership definite.

03

### Documentazione & Supporto

Documenti tecnici obbligatori e affiancamento continuativo all'implementazione.

**CONTATTACI**

[info@tomato.blue](mailto:info@tomato.blue)

**L'AI entra in Azienda senza chiedere permesso. Impara a governarla**

[info@tomato.blue](mailto:info@tomato.blue) · [www.tomato.blue](http://www.tomato.blue)